Identificación, explotación y documentación de una inyección de comandos en DVWA.

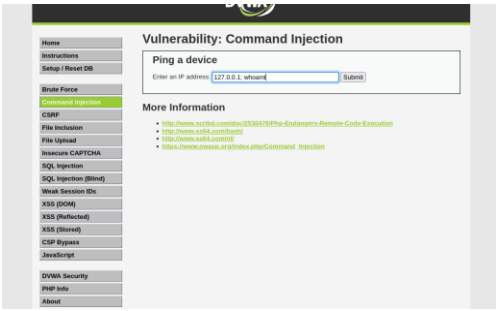
Descripción Técnica del Problema

El módulo "Command Injection" de la aplicación DVWA es vulnerable a la inyección de comandos del sistema operativo. La aplicación no valida ni sanitiza adecuadamente la entrada del usuario en el campo de ping, lo que permite que un atacante inyecte y ejecute comandos arbitrarios del sistema operativo junto con el comando original.

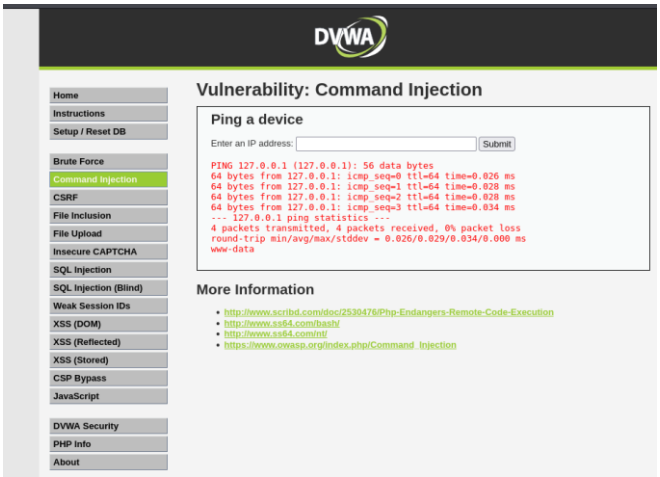
Evidencia

Se utilizaron los siguientes comandos para confirmar la vulnerabilidad y se adjuntan las capturas de pantalla de los resultados:

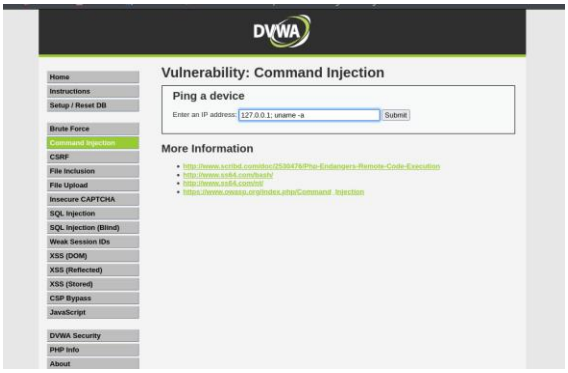
- **Comando de prueba (whoami)**: Se ingresó 127.0.0.1; whoami en el campo de texto.



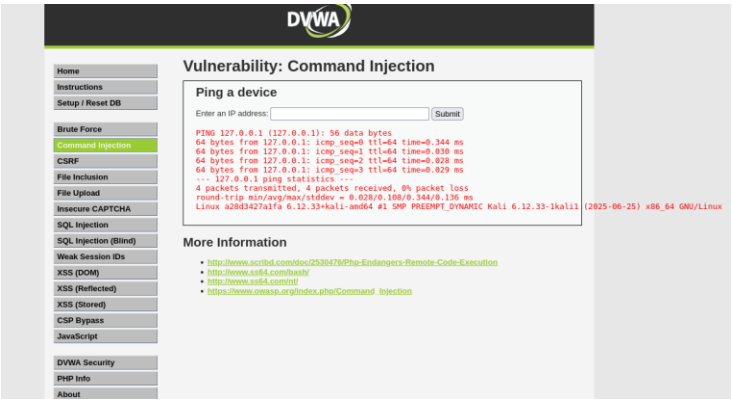
  - **Resultado**: La aplicación devolvió www-data, lo que confirmó que el servidor ejecutó el comando y reveló el usuario con el que se estaba ejecutando el proceso web.



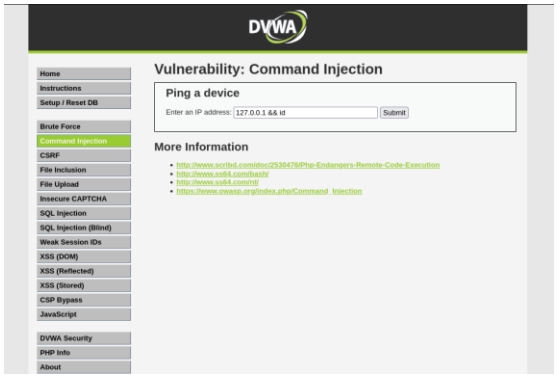
- **Comando avanzado (uname -a)**: Se ingresó 127.0.0.1; uname -a para obtener información del sistema operativo.



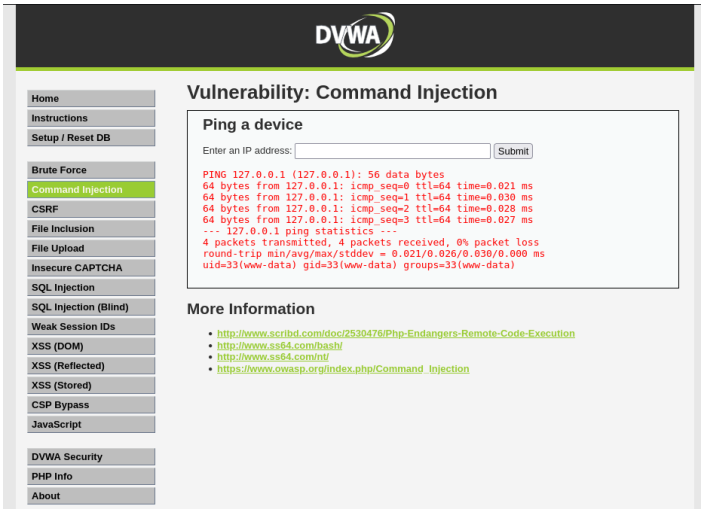
  - **Resultado**: La respuesta del servidor incluyó la versión del kernel y la distribución del sistema operativo: Linux ... Kali ... x86_64. Esto confirma que un atacante puede obtener información detallada del servidor.



- **Comando avanzado (id)**: Se utilizó 127.0.0.1 && id para obtener información sobre el usuario y sus permisos.



  - **Resultado**: Se obtuvo el uid, gid y los grupos del usuario www-data (uid=33(www-data) gid=33(www-data) groups=33(www-data)), lo que brinda información sobre los privilegios del atacante en el sistema.



Evaluación del Riesgo

El riesgo de esta vulnerabilidad se clasifica como **Crítico**. La inyección de comandos otorga a un atacante un control casi total sobre el servidor, lo que le permite:

- **Acceso no autorizado**: Ejecutar comandos con los privilegios del usuario del servidor web.
- **Fuga de datos**: Leer archivos sensibles, como credenciales de bases de datos.
- **Modificación del sistema**: Crear, modificar o eliminar archivos del sistema.
- **Denegación de servicio**: Detener servicios o saturar el sistema con comandos maliciosos.

Recomendación de Mitigación

Para solucionar esta vulnerabilidad y prevenir futuros ataques, se recomienda lo siguiente:

- **Sanitización de Entradas**: Nunca confíes en la entrada del usuario. Se debe filtrar o sanitizar cualquier dato antes de pasarlo a una función del sistema. Es recomendable utilizar una lista blanca que solo permita caracteres y formatos esperados (por ejemplo, solo números y puntos para una IP), y rechace cualquier otro carácter especial (;, &&, |, etc.).
- **Uso de APIs Seguras**: Utiliza funciones o APIs diseñadas para manejar procesos externos de manera segura, sin permitir la inyección de comandos.
- **Privilegios Mínimos**: Asegúrate de que el usuario bajo el cual se ejecuta la aplicación web (www-data en este caso) tenga la menor cantidad de privilegios posible en el sistema.

Referencias

- **OWASP Command Injection**: Documentación oficial sobre la inyección de comandos.
- **CWE-77**: Improper Neutralization of Special Elements used in a Command.
- **CVSS Score**: Una puntuación estimada para este tipo de fallo sería de **9.8 (Crítico)**, ya que permite la ejecución remota de código (RCE).